Two-Hundred and Eighty-first Meeting

Wednesday, 6 March 1985

Defense Intelligence Analysis Center

Bolling Air Force Base

Sanitized Copy Approved for Release 2010/10/07 : CIA-RDP87-00812R000200060041-5

Minutes
Feb

Next 11 Page(s) In Document Denied

AGENDA COMMENTS

PRELIMINARY COMMENTS

TIME SPENT ON SECOM - Chairman, SECOM will remind SECOM members to submit an estimate of the time they spend on SECOM matters to the Chairman, SECOM. PPG has submitted this information, as indicated under Tab A.

UPDATE ON SECURITY AFFAIRS SUPPORT ASSOCIATION (SASA) - General John Morrison has provided a response to Chairman, SECOM's letter stating the Security Committee's negative response to SASA's proposal (attached as Tab B.). General Morrison's response is conciliatory but states that SASA is awaiting response from industry before deciding which why they will go with the proposal.

OGC continues to review the D/OS cable to Agency contractors. [redacted] advises that OGC is researching, at the request of DDS&T, if a conflict of interest exists for Agency personnel who become involved in SASA. OGC has not delivered an opinion on either the cable on the conflict of interest matter to date. STAT

TERMS OF REFERENCE (TOR) FOR COUNTERMEASURES ADVISORY PANEL (CAP) - Chairman, SECOM has forwarded a letter (attached as TAB C) to the Chairman, CAP, [redacted] stating that involvement of the CAP in TSCM matters could result in duplication of effort. If the CAP adopts TOR which eliminate redundant functions, the SECOM and the CAP can mutually support each other according to the memo. C/TSD reports that the CAP meeting on 5 March resulted in disagreement and further attempts by NSA to take over the whole ball of wax. Letter to [redacted] had little, if any, effect according to C/TSD. STAT STAT

ITEM I Approval of Minutes of 8 February Meeting

Action Taken Re Minutes

° UPDATE OF SECOM LEAK DATA BASE - SECOM has been advised that [redacted] of OS/SAG is the Agency nominee to SECOM to update the leak data base as indicated in TAB D. The leak computer fun will be forwarded by SECOM for updating in the near future. STAT

° DEPUTY DIRECTOR/DDS&T LETTER TO SECOM RE LEAKS - Memo from Mr. Hirsch, CIA associate Deputy Director for Science and Technology to C/SECOM (regarding the problem of unauthorized disclosures of classified information through participation of cleared persons in unclassified symposia) has been tasked to

SAG for reporting to SECOM on 29 March. Director of Security cable to contractors and the Hirsch Memo are attached as Tab E.

ITEM 2 Action on proposed change to DCID 1/19 [redacted] will present a Compartmentation Subcommittee proposal to amend section 36 of the Security Policy Manual concerning foreign ownership, control or influence) STAT

° [redacted] will propose only a slight change dealing with the increasing foreign ownership. Basic DCID 1/19 documents are attached as Tab F. STAT

ITEM 3 Draft DCID on TSCM (discussion of DIA, CIA and OSD suggestions for change to the draft DCID to provide policy guidance on technical surveillance countermeasures.)

° There will be a discussion of the draft DCID attached as Tab G. The submission of the C/TSCS is also attached and is the coordinated Agency position submitted to the SECOM. Although COMSEC forwarded their concerns re the DCID to the D/OS COMSEC [redacted] indicated agreement and compliance with the document submitted by C/TSCS. OSD's response has been indicated as negative after review of the TSCS submission and they are expected to be the only ones to vote "no". The draft differs in minor ways from the TSCS submission. The major difference is the inclusion of the disclaimer included in paragraph two under Policy. STAT

ITEM 4 SECOM R&D and procurement projects (discussion of projects proposed for FY-85; suggestions for similar efforts in FY-86 and beyond)

° SECOM tasking re R&D procurement projects and the Agency's response are attached as Tab H.

NEW BUSINESS

° Possibly the nominations for Chairman/UDIS, Chairman/Personnel Security Subcommittee, Chairman/Security Education Subcommittee and for [redacted] replacement will be discussed at this time. Nominations are due to Chairman, SECOM by 15 March. STAT

ITEM 6 Next Meeting - 3 April 1985

Next 2 Page(s) In Document Denied

MEMORANDUM FOR: Chairman, DCI Security Committee

FROM: [redacted] STAT
SECOM Member

SUBJECT: Estimates of Time Spent on SECOM Matters By Members in 1984

1. This memorandum responds to referenced request for information concerning subject.

2. It is estimated that as a SECOM member, I devote approximately five hours per week to SECOM matters, a pattern which prevailed through 1984.

3. The Policy and Plans Group of the Office of Security provides staff support in SECOM matters. It is estimated that, in 1984, one policy officer devoted about 8 working days per month to SECOM activities and required 2 full days per month of secretarial support for those activities.

[redacted] STAT

OS/P&M/PPG/[redacted] (5 Mar 85) STAT
Rewritten: OS/P&M/PPG/[redacted] (6 Mar 85) STAT

Distribution:
Orig - Adse
1 - D/S
1 - OS Registry
1 - PPG Chrono
1 - SECOM File

OS 5 2051

MEMORANDUM FOR: Chairman, DCI Security Committee

FROM: [redacted] STAT
SECOM Member

SUBJECT: Estimates of Time Spent on SECOM Matters By Members in 1984

1. This memorandum responds to referenced request for information concerning subject.

2. It is estimated that as a SECOM member, I devote approximately five hours per week to SECOM matters, a pattern which prevailed through 1984.

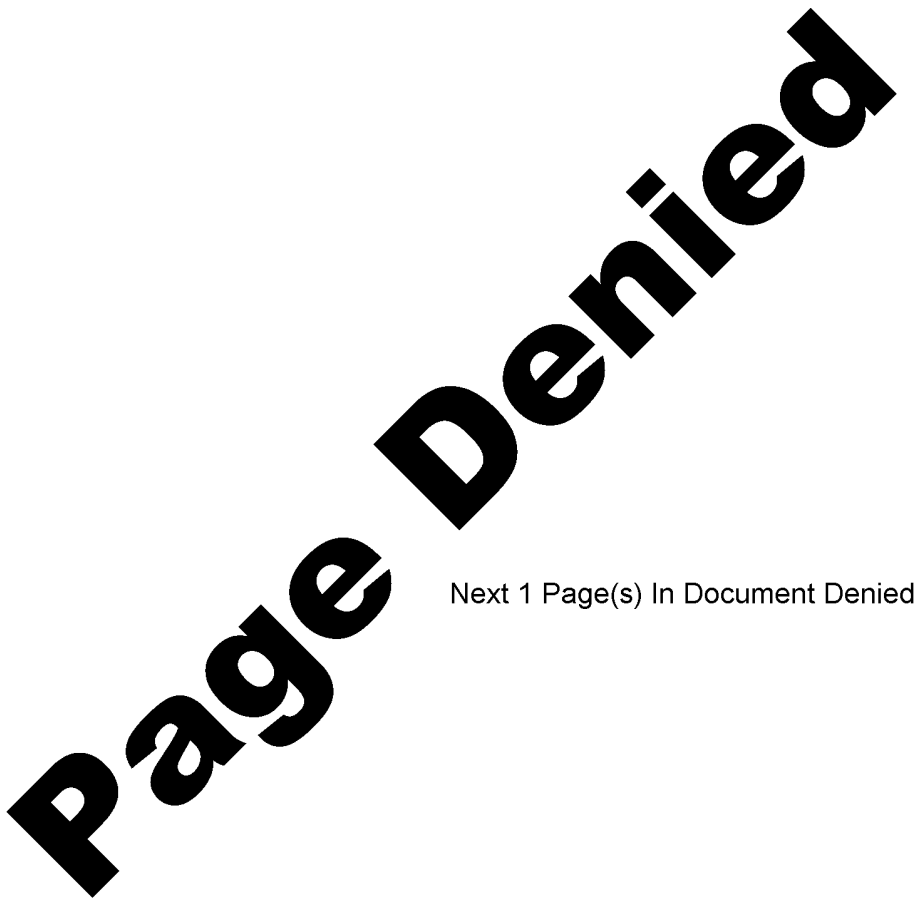
3. The Policy and Plans Group of the Office of Security provides staff support in SECOM matters. It is estimated that, in 1984, one policy officer devoted about 8 working days per month to SECOM activities and required 2 full days per month of secretarial support for those activities.

[redacted] STAT

OS/P&M/PPG/[redacted] (5 Mar 85) STAT
Rewritten: OS/P&M/PPG/[redacted] (6 Mar 85) STAT

Distribution:
Orig - Adse
1 - D/S
1 - OS Registry
1 - PPG Chrono
1 - SECOM File

OS 5 2051



Next 1 Page(s) In Document Denied

[redacted]

ROUTING AND TRANSMITTAL SLIP Date 2/25/85

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. [redacted]		
2.		
3.		
4.		
5.		

STAT

	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS

D/S should see this letter before next SECOM meet - also he should be aware of the status of his message to contractors re SPSB.

Note that the SPSB letter went out to its members on 24 January 85.
(Note contradiction paras 2 and 4)

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
[redacted]	Phone No.

STAT

5041-102

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆ GPO : 1981 O - 341-529 (120)

[redacted]

[redacted]

19 February 1985

FOR: SECOM Members

FROM: Chairman, SECOM

Attached is a copy of a letter received here. It is forwarded for your information.

STAT

[redacted]

DD/P&M

for C/PPG

[redacted]

SASA

THE SECURITY AFFAIRS SUPPORT ASSOCIATION

February 11, 1985

[redacted] STAT

Chairman, DCI Security Committee
Via Ames ISC, Rm. 1225 Ames Building
Washington, D.C. 20505

Dear [redacted] STAT

I am hastening to acknowledge receipt of your letter of 4 February 1985.

I fear that for some reason, perhaps entirely my fault, the SASA proposal has been misunderstood. It was never intended that SASA become involved in any classified aspect of the personnel security clearance program.

Originally, as discussed in our meeting of 11 October we had planned to launch into our study based on encouragement previously and otherwise received. Deferring to the view expressed by you at our meeting, we revised our approach which I described in my letter of 20 November 1984, namely to ask our industry members "as to whether or not they think a SASA program would be helpful." As of 24 January 1985, I dispatched to our members a copy of the letter which was originally enclosed with my letter to you of 20 November 1984.

Your letter of 4 February 1985, suggests "that SASA might wish to reassess the desireability of the proposal". Considering the fact that our letter of 24 January asks our members only to advise us if they "are interested in having SASA undertake a program focused on the resolution of personnel security clearance problems" and that the letter is now in the hands of our members, it would be somewhat awkward for all concerned to retreat at this point. May I respectfully

80 West Street • Suite 110 • Annapolis, Maryland 21401 • (301) 269-5424

[redacted] STAT

suggest that we await the responses to our basic query before we decide the next step.

We may indeed confirm your belief that matters are well in hand and that there is no need for the type of service offered by SASA. Nothing would please us more than to be able to present to you the results of our survey (on a non-attribution basis) confirming that the situation is as you have described it. On the other hand, if contrary views should emerge you would surely wish to be informed. We would intend to do that.

[redacted] we certainly do not wish to engage on this STAT matter in any adversarial manner. If there are any prospects whatsoever of performing a useful service to industry and government, they may only be realized with the cooperation and support of you and the members of your committee whose judgments and authorities we deeply respect.

Please be assured that we continue to be mindful of your concerns and will undertake no action which might have adverse security implications.

Kindest personal regards,

John E. Morrison, Jr.
Major General USAF (Ret.)
Executive Vice President

JEM/cga

[redacted] STAT

It occurs to me that I should also add that SASA now intended to entertain individual cases but only generic problems.

Next 2 Page(s) In Document Denied

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-052
21 February 1985

[redacted] STAT

Chairman
Countermeasures Advisory Panel
S-6, NSA
Ft. Meade, MD 20755

Dear [redacted] STAT

I appreciated the opportunity to meet with you on 15 February 1984 and brief you on some of the activities of the DCI Security Committee. Our Technical Surveillance Countermeasures Subcommittee has, for many years, served as a source of policy formulation, a forum for Intelligence Community discussion of conceptual and practical considerations, and a central coordinating mechanism for technical surveillance countermeasures (TSCM).

The discussion demonstrated that involving the Countermeasures Advisory Panel in TSCM matters could result in duplication of effort and diffusion of the energies of the relatively few TSCM specialists in the government. SECOM, with its subcommittee infrastructure, has been a source of policy on physical security, and has fostered research and development in a broad range of security disciplines. Duplication of such efforts by other interagency groups poses the possibility of further redundancy.

If the CAP adopts terms of reference which eliminate redundant functions, I am confident that we can ensure appropriate exchanges of information and requirements between the CAP and SECOM. We would welcome continuing the dialogue on mutual support. Please feel free to call me.

Sincerely,

[redacted] STAT

cc: OSD Member
CIA Member
C/TSCS

[redacted] STAT

MEMORANDUM FOR: Chairman, DCI Security Committee

FROM: [redacted] 25X1
CIA Member

SUBJECT: Nominee to Update the SECOM Leak Data Base [redacted] 25X1

1. This memorandum is in response to Chairman, SECOM's request that this Agency nominate a representative to update the SECOM data base for unauthorized disclosures. [redacted] 25X1

2. This Agency has nominated [redacted] to serve in this capacity. [redacted] can be contacted through the Office of Security, Security Analysis Group [redacted] 25X1 25X1 25X1

[redacted] 25X1

!OS/P&M/PPG/[redacted](5 Mar 85)! 25X1

!Distribution:!
! Orig - Adse!
! 1 - D/S!
! 1 - OS Registry!
! 1 - PPG Chrono!

[redacted] 25X1

[redacted]

OFFICE OF THE DIRECTOR 25 FEB 1985

Office of Security

TO: C/SAG/PSI

SUBJECT: SECOM LEAK DATA BASE

PLEASE ASK [redacted] TO HANDLE OUR END OF THIS WITH SECOM. 25X1

[redacted] 25X1

C/PPG

C/PSI

[redacted] 25X1

cc: DD/P&M

[redacted]

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Selection of CIA Representative to Update the SECOM Leak Data Base

FROM: [redacted] EXTENSION [redacted] NO. [redacted] 25X1

DATE 12 February 1985

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. C/Policy Br.	2/13/85		JR	This memorandum contains a recommendation that an individual be selected to work on a SECOM task force to update the SECOM Leak Data Base.
2. C/PPG	2/13			
3. DD/P&M	2/13	2/13		
4. DD/S C/OPS/PSI	14 Feb	2/14		Possibly PSI would want to handle this and/or discuss with DIOS as appropriate. 25X1
5. P/S DD/PSI	14 Feb	2/15		
6. C/SAG.		2/20		
7. C/OPS/PSI DD/PSI.	21 Feb / 21 Feb	2/21 / 2/21		#6. Pls see me at your convenience to discuss. 25X1 DD/PSI
8.				
9. D/S.	22			15 Feb PS SECOM Advised that SECOM in the near future will be sending a computer printout of leaks covering the GAP Oct 83 to Nov 1984. We can work with that and provide SECOM with the data they need OR we may have to complete SECOM's preprinted reporting form. We can do the work on other leaks at SAG. I recommend we nominate [redacted] as our representative to the SECOM TASK FORCE although both he and Larry will complete our requirement in SAG. 25X1
10.				
11.				
12. C/SAG				
13. This is OK. I don't believe we should lend bodies to				
14. SECOM to input the info into their system.				25X1 25X1 25X1

FORM 1-79 610 USE PREVIOUS EDITIONS

GPO : 1983 O - 411-630

MEMORANDUM FOR: Director of Security

VIA: Deputy Director, Policy and Management

FROM: [redacted] 25X1
Policy and Plans Group

SUBJECT: Selection of CIA Representative to Update the SECOM Leak Data Base [redacted] 25X1

1. Chairman, SECOM has requested that this Agency select a representative to a SECOM Task Force to review and update the SECOM Leak Data Base. This individual will work with one representative from the National Security Agency (NSA) and one from the Defense Intelligence Agency (DIA) on this task force. [redacted] 25X1

2. Each of the respective representatives will be expected to review the leak files from his own Agency to update the data base from October 1983 to the present. Much of this work will be done in the individual's normal office location. However, the task force will be required to update the inputs from agencies other than CIA, NSA and DIA that have contributed to the data base. [redacted] 25X1

3. The two officers who are assigned to leak investigations for the Office of Security are [redacted] 25X1 and [redacted] 25X1 It is suggested that the Director of Security select one of these individuals to participate in the proposed task force. [redacted] 25X1

[redacted] 25X1

[redacted] 25X1

CONFIDENTIAL

Next 1 Page(s) In Document Denied

DDS&T-083-85

1 February 1985

MEMORANDUM FOR: Chairman, Security Committee

FROM: James V. Hirsch
Associate Deputy Director for Science and Technology

SUBJECT: Leaks of Classified Information

1. It seems to me that we in government unwittingly aid one of the major sources of leaks of classified information we suffer from today. The source I refer to is the group of self-proclaimed intelligence pundits associated with specialized study centers or institutes. These individuals openly publish or discuss details of our collection sources and analysis results. The ones who can do the most damage are those who have had prior legitimate access to classified information. This inside knowledge is often used to pick selectively from the media that information that is very close to the truth for use in public unclassified papers or discussions. In this way erroneous data are gradually sifted out of these analysts' treatment a given classified issue. Some of these analysts have been careful to identify prior open sources for their specific studies. I know of one case of a strategic analyst, a foreigner, who managed to associate himself with U.S. think-tanks and, by insinuation of SCI access, managed to elicit classified information in his discussions. Recently, a subpanel on technical collection of intelligence of an unclassified symposium on strategic issues advertised the participation of an individual who used to work with one of our contractors and who held a number of our SCI clearances.

2. The currency of this particular source of intelligence leakage constantly decays without access to inside information. If we could isolate these sources of leaks from so-called unclassified governmental or government contractor interaction, their effectiveness would be significantly diminished. It doesn't make sense for one part of the government to rail against intelligence leakage while other parts cheerfully participate in open forums with individuals who systematically use such exchanges to confirm or deny classified information already in the public domain. It would seem prudent for us to investigate ways in which we can prevent government and government contractor participation in unclassified conferences when there is a risk that by doing so we could aid in verifying the accuracy of intelligence information appearing in unclassified published materials. We gain little or nothing of substance from many of these exchanges, especially when technical collection of intelligence is the topic. Would it be possible

25X1

CONFIDENTIAL

SUBJECT: Leaks of Classified Information

for your committee to develop guidelines to limit the participation of Intelligence Community organizations and their contractors in unclassified symposia, conferences or technical meetings dealing with intelligence when such participation could aid in establishing the credibility of known leakers of classified information?

25X1

James V. Hirsch

CONFIDENTIAL

Next 11 Page(s) In Document Denied

1 FEB 1985

MEMORANDUM FOR: Chairman, DCI Security Committee

FROM: [redacted] STAT
CIA Member

SUBJECT: Proposed DCID on Technical Security Countermeasures

REFERENCE: SECOM D-299, dated 21 December 1984

1. This memorandum responds to referenced request for comments regarding subject.

2. The Chairman, SECOM Technical Security Countermeasures Subcommittee (TSCS), has provided his comments directly to the Chairman.

3. Representatives of this Agency's Office of Communications (COMSEC) have reviewed the reference and the TSCS document. COMSEC is in concurrence with the TSCS submission to SECOM.

/Signed/

[redacted] STAT

!OS/P&M/PPG/[redacted] (25 Jan 85)! STAT

!Distribution:!
!Orig - Adse!
! 1 - D/S!
! 1 - PPG Chrono!
! 1 - OS Reg!

OS 5 2021

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

DRAFT DCID Technical Surveillance Countermeasures

FROM:	EXTENSION	NO.
		DATE

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. PPG	4 Jan 85		MVW	Per our conversation, this is a copy of what we forwarded to SECOM.
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

STAT

STAT

FORM 1-79 610 USE PREVIOUS EDITIONS

GPO : 1983 O - 411-632

MEMORANDUM FOR: CHAIRMAN, SECURITY COMMITTEE

FROM: Chairman, Technical Surveillance Countermeasures Subcommittee

SUBJECT: DRAFT DCID Technical Surveillance Countermeasures

REFERENCE: SECOM D-299

1. The referenced draft DCID was discussed in depth at the TSCS meeting held on 17 January. It was a consensus of the members that the draft DCID should be modified as follows: Changes are underlined for ease of comparison.

Pursuant to the provisions of Section 102 of the National Security Act of 1947 and Executive Order 12333, and National Security Decision Directive Number 145 which affirms the role of the Director of Central Intelligence as executive agent for the Intelligence Community and advisor to the U.S. Government for technical surveillance countermeasures (TSCM), this directive establishes policy and procedures for the conduct and coordination of TSCM within the Intelligence Community.

1. Purpose

This directive assigns responsibilities to the Intelligence Community and provides guidance to other U.S. Government organizations for TSCM to prevent the compromise or loss of national security information through the use of technical surveillance.

2. Policy

U.S. Government departments and agencies which handle classified and other sensitive national security information shall conduct or arrange for TSCM activities in accordance with Director of Central Intelligence (DCI) guidance.

3. Definitions

a. Technical Surveillance Countermeasures (TSCM) are techniques and measures to detect and neutralize a wide variety of hostile penetration technologies which are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic and acoustic means, as the

25X1

sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. TSCM also includes the development and use of protective systems to detect and deter hostile penetration attempts and the hostile exploitation of naturally occurring hazards. These measures include systems to protect telephones, secure conference rooms and office areas, and the safeguard of various classified information handling and storage equipments.

b. The Intelligence Community comprises those U.S. Government agencies and organizations so identified in Executive Order 12333.

4. Responsibilities

a. The DCI Security Committee shall:

(1) Advise and assist the DCI on the establishment of policy and procedural guidance covering TSCM activities for the U.S. Government. This shall include prepartaion of written guidance for the Intelligence Community on the conduct of TSCM inspections, coordination of action concerning identified penetration devices and security hazards in U.S. equipment, and timely dissemination of information on TSCM.

(2) Coordinate the development and use of the most effective means for protecting national security information against technical surveillance.

(3) Establish subordinate subcommittees and working groups to address specific aspects of TSCM.

(4) Develop arrangements with Intelligence Community agencies for the provision of services of common concern in areas such as TSCM training, security analysis of telephone equipment and testing and analysis of penetration devices used against the U.S. Government or other nations. Coordinate the conduct of those services.

(5) Coordinate Intelligence Community research and development programs on TSCM.

(6) Promote and foster joint procurement of TSCM equipment by Intelligence Community agencies.

(7) Evaluate the impact on national security of proposed foreign disclosure of TSCM equipment or techniques, and recommend policy changes as needed.

(8) Prepare collection guidance for Intelligence Community use in obtaining intelligence information on the plans, capabilities and actions of foreign governments concerning technical penetrations and countermeasures against them.

b. Intelligence Community departments and agencies shall:

(1) Conduct TSCM inspections in accordance with established DCI Procedural Guides.

(2) Report to the DCI Security Committee, data obtained on the technical surveillance threat and on penetration devices and techniques used against the United States or other nations.

(3) Disseminate within their areas of responsibility all-source collection guidance on TSCM and ensure that intelligence collected is provided to the DCI Security Committee.

(4) Ensure that the DCI Security Committee is kept appraised of their TSCM training and research and development requirments and activities.

(5) Assist one another to the extent of their capabilities through the provision of services of common concern and shared research and development efforts.

(6) Provide TSCM support to U.S. Government departments and agencies outside the Intelligence Community in accordance with memoranda of understanding or other agreements.

(7) Coordinate through the DCI Security Committee proposed foreign disclosure of TSCM equipment or techniques.

c. Other U.S. Government departments and agencies may:

(1). Arrange for TSCM support from Intelligence Community member organizations through memoranda of understanding or other forms of agreement. These shall be coordinated with the DCI Security Committee.

2. If you have any further questions about the above or require any additional information please telephone me on [redacted] 25X1

25X1

[redacted]

CONFIDENTIAL

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-299

21 December 1984

MEMORANDUM FOR: SECOM Members

FROM: [redacted] 25X1
Chairman

SUBJECT: **Policy on Technical Surveillance Countermeasures** [redacted] 25X1

1. Attached for your review is a draft Director of Central Intelligence Directive to provide policy guidance on technical surveillance countermeasures (TSCM). There is a need for specific guidance in this area. NSDD-145 states in paragraph 10a that nothing in that directive alters existing DCI authorities as Executive Agent of the Government for TSCM. Those authorities need to be spelled out to ensure common understanding of areas of responsibility. The SECOM charter does not provide any degree of specificity in that regard. [redacted] 25X1

2. This draft directive will be discussed at the 9 January 1985 SECOM meeting. Please come prepared to comment on it. [redacted] 25X1

[redacted] 25X1

Attachment: a/s

cc: Chairman, SECOM TSCS, w/att

[redacted] 25X1

CONFIDENTIAL

Next 3 Page(s) In Document Denied

CONFIDENTIAL

14 Jan 85
*OC-0045

MEMORANDUM FOR: Director of Security

FROM: [redacted] 25X1
Director of Communications

SUBJECT: Proposed DCI Directive on TSCM [redacted] 25X1

1. As has been informally discussed between our Staffs, and as a follow-on to discussions at the 9 January 1985 SECOM meeting, I would like to document my concerns regarding the proposed DCI Directive on Technical Surveillance Countermeasures (TSCM). While the initiative to establish DCI guidance in light of NSDD 145 is understood, it is believed that portions of the proposed broad definition of TSCM overlap substantially with [redacted] 25X1

3. The following additional comments are suggested:

[redacted] 25X1

SUBJECT: Proposed DCI Directive on TSCM [redacted] 25X1

4. It is recommended that our Staffs schedule a meeting to discuss the above concerns and comments to determine how best to incorporate them into the proposed DCID. [redacted] 25X1
[redacted] is the OC Point of Contact. [redacted] 25X1

/s/ 25X1
[redacted]

OMIC:DC/OC-CSD [redacted] (11 JAN 85) 25X1

Distribution:
Original - Addressee
1 - OC-CSD/TSG, w/att.
1 - DC-CSD
1 - OC-CSD Chrono

AUTH:

/s/ 11 Jan 85
Chief, OC-CSD Date

ROUTING AND RECORD SHEET

SUBJECT: (Optional)
FY 85 R&D and Procurement Candidate Projects

FROM:

NO. 25X1

DATE 13 March 1985

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. C/Policy Br.	3/13/85		JR	Attached is response to SECOM tasking regarding subject.
2. C/PPG	3/13/85		MKW	
3. DD/P&M	3/13/85		D	
4. ~~DD/S~~				
5. ~~D/S~~				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				

25X1

FORM 1-79 **610** USE PREVIOUS EDITIONS

CONFIDENTIAL

GPO : 1983 O - 411-632

14 MAR 1985

MEMORANDUM FOR: Chairman, SECOM

FROM: [redacted] STAT
SECOM Member

SUBJECT: FY 85 R&D and Procurement Candidate Projects

1. This memorandum is in response to a request from Chairman, SECOM, to provide comments concerning the list of SECOM Contract Projects for FY 1985 provided to the membership at the 6 March 1985 SECOM meeting.

2. The listing, as indicated, meets with my approval. It is my observation that the "Study of How Leaks Distort the Criminal Justice System in Graymail Cases" seems to be an obscure topic that does not have sufficient broad-based interest to be included, but this is only an observation and not a negative response to conducting such a study.

[redacted] STAT

!OS/P&M/PPG [redacted] (13 Mar 85)! STAT

!Distribution:!
! Orig - Adse!
! 1 - D/S!
! 1 - OS Registry!
! 1 - PPG Chrono!
(1) - SECOM File

OS 5 2057